UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/408,420	09/29/1999	SUNIL K. SRIVASTAVA	50325-076	4033

29989 7590 02/10/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/408,420	SRIVASTAVA, SUNIL K.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *04/04, 11/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on July 09, 2004. Original application contained Claims 1-30. Applicant previously added Claims 46-61. Applicant currently amended Claims 1-5, 8-15, 18-24, 26-28, 31, and added new claims 32-80. Therefore, presently pending claims are 1-80.

Response to Arguments

Applicant's arguments with respect to claims 1-30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-80 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Mittra (U. S. Patent 5,748736), and further in view of Squire et al. (U. S. Patent 6,745,243).

3. Regarding Claim 1 Mittra teaches and describes a method for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a plurality of group controllers, wherein each group controller of the plurality of group controllers is a replica of a particular group controller, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers (Fig.1-3, col.6 line 4 to line 45), the method comprising the steps of:

joining a first group controller to the plurality of group controllers in a local network (col.7 line 45 to line 51);

establishing, a secure communication channel between the first group controller and second controller of the plurality of group controllers using a key exchange protocol (col.7 line 52 to line 60);

receiving a request to add or delete a network node of the secure multicast or broadcast group from a load balancer that is coupled to the plurality of group controllers (col.7 line 64 tocol.8 line 50);

creating and storing a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group (col.8 line 45 to line 67) ; and

distributing a group session key from a third group controller of the plurality of group controller to the network nodes (col.8 line 51 to line 67).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

4. Regarding Claim 11 Mittra teaches and describes computer-readable medium for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a plurality of group controllers, wherein each group controller of the plurality of group controllers is a replica of a particular group controller, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, and which instructions, when executed by one or more processors, cause the processors to carry out the steps of (Fig.1-3, col.6 line 4 to line 45):

joining a first group controller to the plurality of group controllers in a local network (col.7 line 45 to line 51);

establishing, a secure communication channel between the first group controller and second controller of the plurality of group controllers using a key exchange protocol (col.7 line 52 to line 60);

receiving a request to add or delete a network node of the secure multicast or broadcast group from a load balancer that is coupled to the plurality of group controllers (col.7 line 64 tocol.8 line 50);

creating and storing a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group (col.8 line 45 to line 67); and

distributing a group session key from a third group controller of the plurality of group controller to the network nodes (col.8 line 51 to line 67).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

5. Regarding Claim 21 Mittra teaches and describes a method of managing addition and deletion of network nodes form and to a secure multicast or broadcast group of network nodes in a communications network, wherein each of the network nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers (Fig.1-3, col.6 line 4 to line 45), the method comprising the steps of:

joining the first group controller in a local network in which the plurality of group controllers are coupled (col.7 line 45 to line 51, and col.13 line 39 to line 44);

establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange (col.7 line 52 to line 60, and col.13 line 45 to line 53);

receiving a request to add or delete a network node from a load balancer that controls distribution of requests to the plurality of group controllers (col.7 line 64 tocol.8 line 50, and col.13 line 24 to line 35);

generating a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group (col.8 line 4 to line 67); and

distributing the group session key from the first group controller to the other group controllers of the plurality of group controllers over the secure channel (col.8 line 51 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

6. Regarding Claim 24 Mittra teaches and describes a method for creating a secure multicast or broadcast group (Fig.1-3), the method comprising the steps of,

establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol (col.7 line 52 to line 60, and col.13 line 45 to line 53);

load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers (col.7 line 64 tocol.8 line 50, and col.13 line 24 to line 35); and

distributing a group session key by one of the group controllers based upon a logical arrangement of the network nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of network nodes correspond to leaf nodes of the binary tree structure and the plurality of group controllers correspond to the root node channel (col.8 line 4 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to

discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

7. Regarding Claim 31 Mittra teaches and describes a computer system that can manage addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a plurality of group controllers, wherein each group controller of the plurality of group controllers is replica of a particular group controller, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, (Fig.1-3, col.6 line 4 to line 45) the computer system comprising:

- a load balancer coupled to the plurality of group controllers for interfacing inbound service requests to a selected group controller of the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35);

- a bus coupled to the load balancer for transferring data;

- one or more processors coupled to the bus for selectively generating a group session key under control of program instructions, a memory coupled to the one or more processors via the bus, one or more sequences of program instructions stored in the memory which, when executed by the one or more processors cause the one or more is processors (col.6 line 45 to line 61) to perform the steps of:

joining a first group controller to the plurality of group controllers in a local network (col.7 line 45 to line 51, and col.13 line 39 to line 44);

establishing, a secure communication channel between the first group controllers and second group controller of the plurality of group controller using a key exchange protocol (col.7 line 52 to line 60, and col.13 line 45 to line 53);

receiving a request to add or delete a network node of the secure multicast or broadcast group from the load balancer that is coupled to the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35);

creating and storing a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group (col.8 line 4 to line 67); and

distributing the group session key from a third group controller of the plurality of group controllers to the network nodes channel (col.8 line 51 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

8. Regarding Claim 41, Mittra teaches and describes apparatus for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a plurality of group controllers, wherein each group controller of the plurality of group controllers is a replica of a particular group controller, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the

binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers (Fig.1-3, col.6 line 4 to line 45), the apparatus comprising:

means for joining a first group controller to the plurality of group controllers in a local network (col.7 line 45 to line 51, and col.13 line 39 to line 44);

means for establishing a secure communication channel between the first group controller and a second group controller of the plurality of group controllers using a key exchange protocol (col.7 line 52 to line 60, and col.13 line 45 to line 53);

means for receiving a request to add or delete a network node of the secure multicast or broadcast group from a load balancer that is coupled to the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35);

means for creating and storing a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group (col.8 line 4 to line 67); and

means for distributing a group session key from a third group controller of the plurality of group controllers to the network nodes channel (col.8 line 51 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently

manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

9. Regarding Claim 51, Mittra teaches and describes a computer-readable medium comprising one or more sequences of instructions for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network, wherein each of the network nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality

of group controllers, and which instructions, when executed by one or more processors (Fig.1-3, col.6 line 4 to line 45), cause the processors to carry out the steps of:

joining the first group controller in a local network in which the plurality of group controllers are coupled (col.7 line 45 to line 51, and col.13 line 39 to line 44);

establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange (col.7 line 52 to line 60, and col.13 line 45 to line 53);

receiving a request to add or delete a network node from a load balancer that controls distribution of requests to the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35);

generating a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group (col.8 line 4 to line 67); and

distributing the group session key from the first group controller to the other group controllers of the plurality of group controllers over the secure channel (col.8 line 51 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and

network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

10. Regarding Claim 54, Mittra teaches and describes a computer-readable medium comprising one or more sequences of instructions for creating a secure multicast or broadcast group, and which instructions, when executed by one or more processors (Fig.1-3, col.6 line 4 to line 45), cause the processors to carry out the steps of:

establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol (col.7 line 52 to line 60, and col.13 line 45 to line 53);

load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35); and

distributing a group session key by one of the group controllers based upon a logical arrangement of the network nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of network nodes correspond

to leaf nodes of the binary tree structure and the plurality of group controllers correspond to the root node (col.8 line 4 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

11. Regarding Claim 61, Mittra teaches and describes a computer system that can manage addition and deletion of network nodes from and to a secure multicast or broadcast group of

network nodes in a communications network, wherein each of the network nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers (Fig.1-3, col.6 line 4 to line 45), the computer system comprising:

joining the first group controller in a local network in which the plurality of group controllers are coupled (col.7 line 45 to line 51, and col.13 line 39 to line 44);

establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange (col.7 line 52 to line 60, and col.13 line 45 to line 53);

receiving a request to add or delete a network node from the load balancer that controls distribution of requests to the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35);

generating a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group (col.8 line 4 to line 67); and

distributing the group session key from the first group controller to the other group controllers of the plurality of group controllers over the secure channel (col.8 line 51 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4), wherein

a load balancer coupled to the plurality of group controllers for interfacing inbound service requests to a selected group controller of the plurality of group controllers, a bus coupled to the load balancer for transferring data, one or more processors coupled to the bus for selectively generating a group session key under control of program instructions, a memory coupled to the one or more processors via the bus (col.4 line 61 to col.5 line 10,and col.8 line 4 to line 33);

one or more sequences of program instructions stored in the memory which, when executed by the one or more processors cause the one or more processors to perform the steps (col.9 line 58 to col.10line 20) mentioned above

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network

session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

12. Regarding Claim 64, Mittra teaches and describes a computer system that can create a secure multicast or broadcast group, the

computer system comprising:

establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol (col.7 line 52 to line 60, and col.13 line 45 to line 53);

load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35); and

distributing a group session key by one of the group controllers based upon a logical arrangement of the network nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of network nodes correspond to leaf nodes of the binary tree structure and the plurality of group controllers correspond to the root node (col.8 line 4 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4), wherein:

a load balancer coupled to the plurality of group controllers for interfacing inbound service requests to a selected group controller of the plurality of group controllers, a bus coupled to the load balancer for transferring data, one or more processors coupled to the bus for selectively generating a group session key under control of program instructions, a memory coupled to the one or more processors via the bus (col.4 line 61 to col.5 line 10,and col.8 line 4 to line 33);

one or more sequences of program instructions stored in the memory which, when executed by the one or more processors cause the one or more processors to perform the steps (col.9 line 58 to col.10line 20) mentioned above

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also

provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

13. Regarding Claim 71, Mittra teaches and describes an apparatus for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network, wherein each of the network nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group (Fig.1-3, col.6 line 4 to line 45), intermediate nodes,
represent other network nodes, and root nodes represent the plurality of group
controllers, the apparatus comprising:
means for joining the first group controller in a local network in which the plurality of group controllers are coupled (col.7 line 45 to line 51, and col.13 line 39 to line 44);
means for establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange (col.7 line 52 to line 60, and col.13 line 45 to line 53);
means for receiving a request to add or delete a network node from a load balancer
that controls distribution of requests to the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35);
means for generating a new group session key for each network node represented in

each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group (col.8 line 4 to line 67); and means for distributing the group session key from the first group controller to the other group controllers of the plurality of group controllers over the secure channel (col.8 line 51 to line 67, and col.13 line 60 to col.14 line 10).

14. Regarding Claim 74, Mittra teaches and describes an apparatus for creating a secure multicast or broadcast group (Fig.1-3, col.6 line 4 to line 45), the apparatus comprising:

means for establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol (col.7 line 52 to line 60, and col.13 line 45 to line 53);

means for load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers (col.7 line 64 to col.8 line 50, and col.13 line 24 to line 35); and

means for distributing a group session key by one of the group controllers based upon a logical arrangement of the network nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of network nodes correspond to leaf nodes of the binary tree structure and the plurality of group controllers correspond to the root node (col.8 line 4 to line 67, and col.13 line 60 to col.14 line 10).

Although the system disclosed by Mittra shows all the features of the claimed limitation, but Mittra does not specifically disclose load balancer in network environment to mange the network traffic.

In an analogous art, Squire, on the other hand discloses computing environment where load balancing devices have been added to networks components in an effort to more efficiently manage the finite bandwidth of the network capacity, and a load balancing device is designed to route network traffic through optimal data paths based on a number of traffic-centric and network-centric parameters, in accordance with a network management strategy (col.7 line 53 to col.8 line 4).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Mittra and Squire, because Squire's optimized method to discriminate network traffic based on network session information for selecting traffic to determining network routing, would not only analyzes network traffic to identify network session information and based on the network session information network performing load balancing in accordance with a predetermined network management strategy, but will also provide an integrated network load balancer, wherein controller load balancing device is implemented as a front end for a collection of servers.

8. Claims 2, 3, 5, 7, 9, 12, 13, 15, 17, 19, 22, 25, 26, 28, 30, 32, 33, 35, 37, 39, 42, 43, 45, 47, 49, 52, 55, 56, 58, 60, 62, 65, 66, 68, 70, 72, 75, 76, 78, and 80 are rejected applied as above rejecting Claims 1, 11, 21, 24, 31, 41, 51, 54, 61, 64, 71, and 74. Furthermore, the system of Mittra and Squire teaches and describes

- distributing a group session key further comprises: receiving a token value at the third group controller to designate the third group controller as having permission to selectively generate the group session key and to generate node keys associated with the intermediate nodes

and the leaf nodes; and creating and storing the group session key only when the group controller has the token value (col.2 line 8 to line 20);

- distributing a group session key further comprises: determining whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group, determining which of the intermediate nodes are affected by the leaving node, updating keys associated with the affected intermediate nodes, generating a new group session key, and sending the new group session key to the leaf nodes (col.8 line 36 to line 67);

- distributing a group session key further comprises: receiving a request message from one of the network nodes to join the secure multicast or broadcast group, determining which of the intermediate nodes are affected by the joining node, updating keys associated with the affected intermediate nodes; generating a new group session key and a private key of the joining node; and sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node (col.7 line 26 to col.8 line 35).

- receiving a request comprises receiving the request at a load balancer having a single virtual address that represents the plurality of group controllers, and establishing a secure communication channel comprises exchanging a public key of the first group controller with all other group controllers in the plurality of group controllers based upon optimized broadcast Diffie-Hellman protocol (col.6 line 3 to line 61).

- distributing a group session key further comprises: receiving a token value at the group controller to designate the group controller as having permission to selectively generate the group session key and to generate node keys associated with the intermediate nodes and the leaf

nodes; and creating and storing the group session key only when the group controller has the token value (col.2 line 8 to line 20).

- distributing a group session key further comprises: determining whether the secure multicast or broadcast group has a node that is leaving the secure multicast or broadcast group, determining which of the intermediate nodes are affected by the leaving node, updating keys associated with the affected intermediate nodes, generating a new group session key; and sending the new group session key to the leaf nodes (col.8 line 36 to line 67).

- distributing a group session key further comprises: receiving a request message from one of the plurality of nodes to join the secure multicast or broadcast group, determining which of the intermediate nodes are affected by the joining node; updating keys associated with the affected intermediate nodes; generating a new group session key and a private key of the joining node; and sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node (col.7 line 26 to col.8 line 35).

- the steps of generating the group session key only when the first group controller is designated as a master group controller that is authorized to join nodes and generate group session keys (col.12 line 50 to col. 13 line 18);

- step of distributing further comprises: circulating a token among the plurality of group controllers to designate the one group controller as having permission to selectively generate the group session key and keys associated with the intermediate nodes and the leaf nodes; and selectively generating the group session key based upon the circulating step (col.2 line 8 to line 20, and col.13 line 39 to line 56)

- addressing the plurality of group controllers using a single virtual address (col.6 line 3 to line 61, and col.4 line 56 to col. 5 line 12).

9. Claims 4, 6, 8, 10, 14, 16, 18, 20, 23, 27, 29, 34, 36, 38, 40, 44, 46, 48, 50, 53, 57, 59, 63, 67, 69, 73, 77, and 79 are rejected applied as above rejecting claims 3, 5, 7, 13, 15, 17, 22, 26, 28, 33, 35, 37, 43, 45, 47, 52, 56, 58, 62, 66, 68, 72, 76, and 78. Furthermore, Mittra teaches and describes a system and method, wherein:

- updating keys comprises: generating a new key of a parent node of the leaving node; and encrypting the new key of the parent node with a key of a network node adjacent to the parent node, and updating keys comprises performing a one way hash function on the keys associated with the affected intermediate nodes (col. 8 line 37 to line 67,and col. 13 line 59 to line 67);

- the step of load balancing network traffic that is directed from a plurality of the network nodes to the plurality of group controllers (col.12 line 50 to col.13line 18);

- establishing a secure communication channel comprises: receiving a public key value that is broadcast by the Joining node, sending a collective public key value from the network nodes to the joining node, computing a shared secret key; and creating and storing a group shared secret key by exchanging private key values (col.12 line 60 to col.13 line 18);

- the steps of successively designating different ones of the group controllers as the master group controller in real time (col.12 line 50 to col.13 line 18).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

sz
January 28,2005

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER